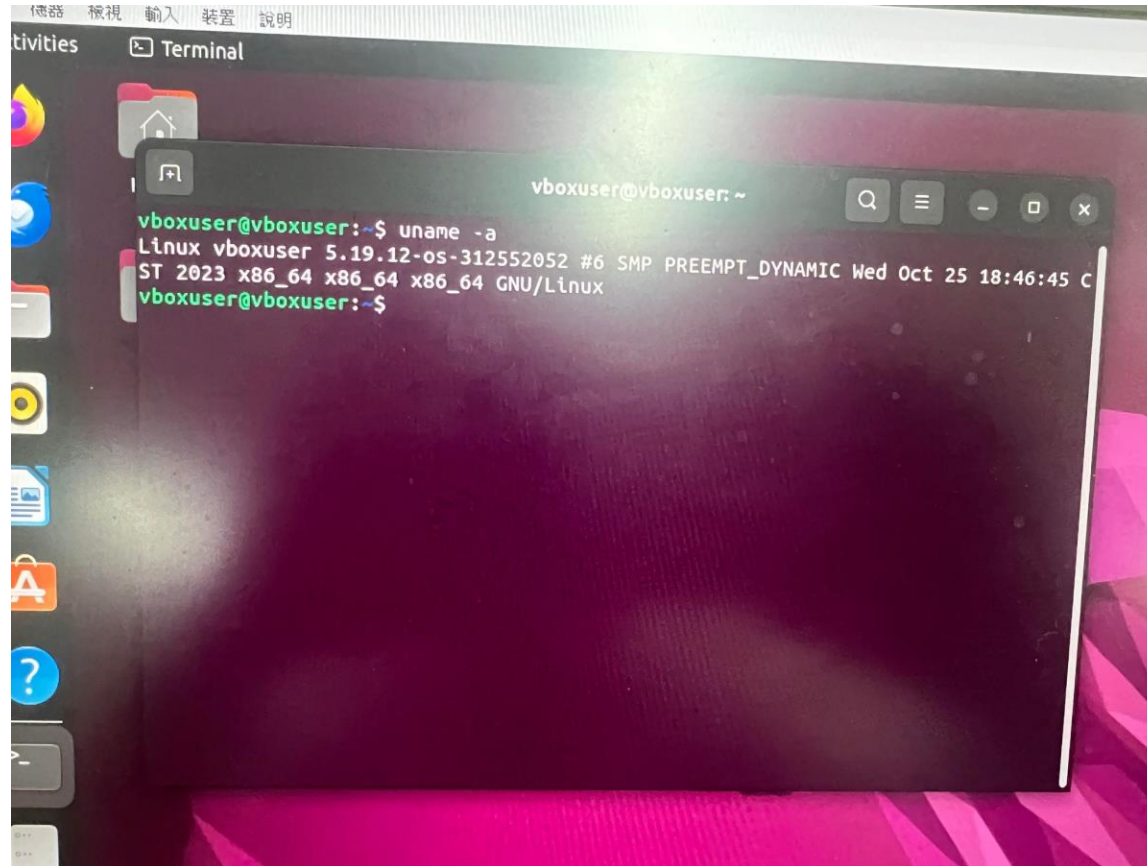


1. 創建一個虛擬機, 分配10核心與50GB



2.change kernel suffix



The image shows a terminal window on a Linux desktop. The window title is "Terminal". The prompt is "vboxuser@vboxuser: ~". The command "uname -a" has been executed, and the output is displayed on the next line. The output string is "Linux vboxuser 5.19.12-os-312552052 #6 SMP PREEMPT_DYNAMIC Wed Oct 25 18:46:45 CST 2023 x86_64 x86_64 x86_64 GNU/Linux".

```
vboxuser@vboxuser: ~  
vboxuser@vboxuser:~$ uname -a  
Linux vboxuser 5.19.12-os-312552052 #6 SMP PREEMPT_DYNAMIC Wed Oct 25 18:46:45 CST 2023 x86_64 x86_64 x86_64 GNU/Linux  
vboxuser@vboxuser:~$
```

執行中] - Oracle VM VirtualBox

機器 檢視 輸入 裝置 說明

Activities Terminal



vboxuser@vboxuser: ~



```
vboxuser@vboxuser:~$ cat /etc/os-release
```

```
PRETTY_NAME="Ubuntu 22.04.3 LTS"
```

```
NAME="Ubuntu"
```

```
VERSION_ID="22.04"
```

```
VERSION="22.04.3 LTS (Jammy Jellyfish)"
```

```
VERSION_CODENAME=jammy
```

```
ID=ubuntu
```

```
ID_LIKE=debian
```

```
HOME_URL="https://www.ubuntu.com/"
```

```
SUPPORT_URL="https://help.ubuntu.com/"
```

```
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
```

```
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
```

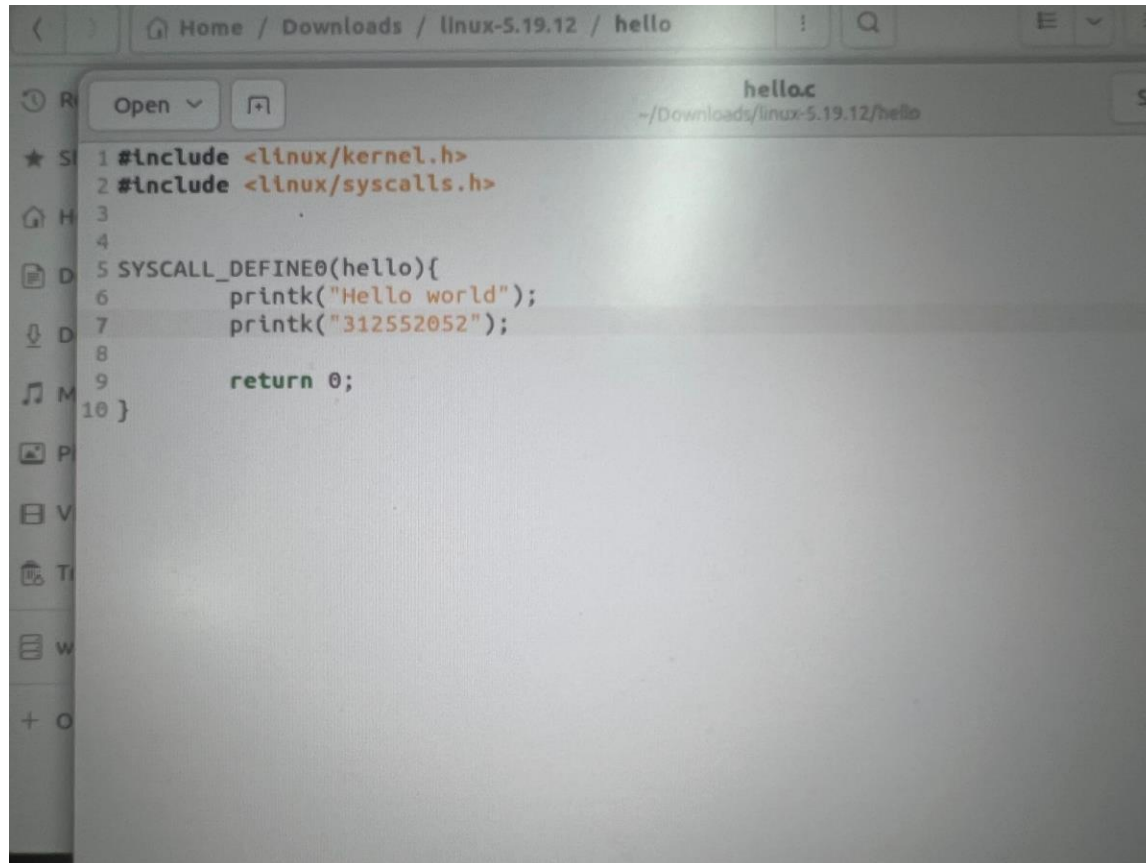
```
UBUNTU_CODENAME=jammy
```

```
vboxuser@vboxuser:~$
```

3.建一個hello資料夾

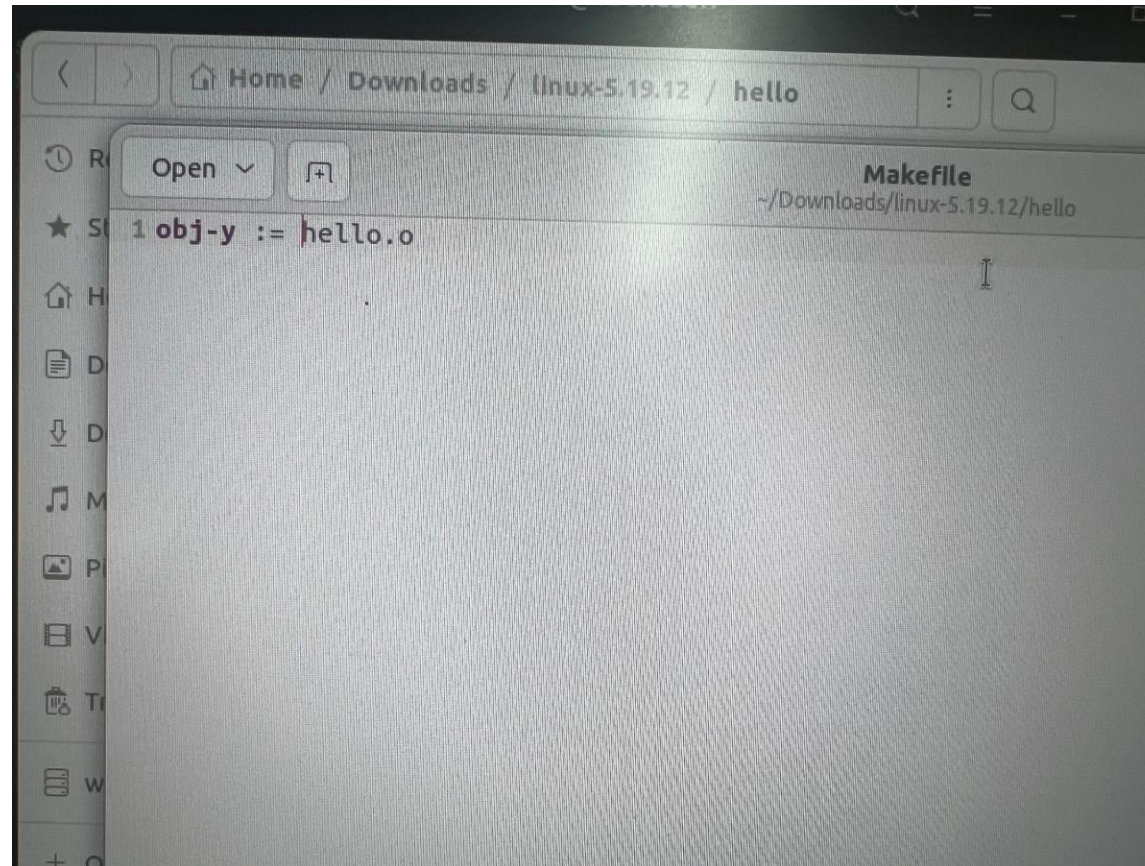
- Mkdir hello.

4. 寫入hello.c file

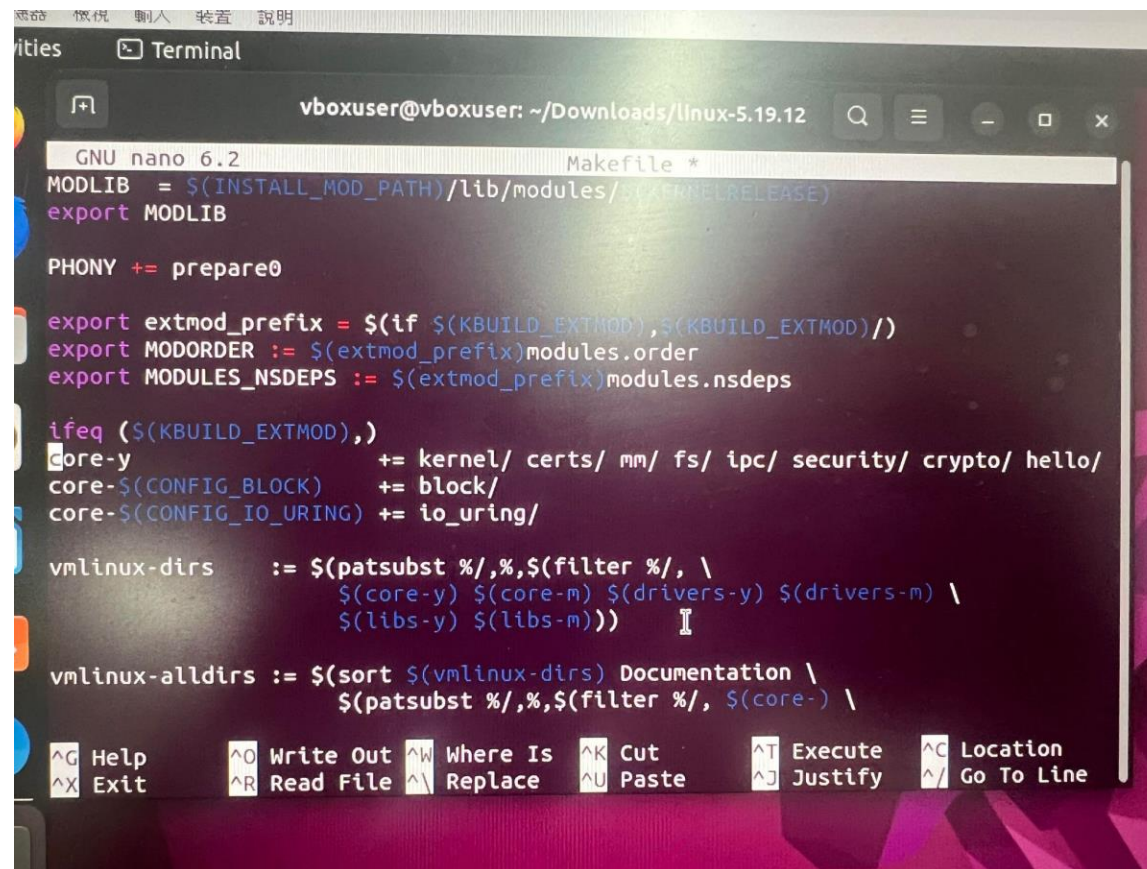


```
1 #include <linux/kernel.h>
2 #include <linux/syscalls.h>
3
4
5 SYSCALL_DEFINE0(hello){
6     printk("Hello world");
7     printk("312552052");
8
9     return 0;
10 }
```

5.create a makefile



6. 搜尋makefile 之 core-y 更改



The image shows a terminal window with a nano editor editing a Makefile. The terminal title bar indicates the user is 'vboxuser' at 'vboxuser: ~/Downloads/linux-5.19.12'. The nano editor's status bar at the top shows 'GNU nano 6.2' and 'Makefile *'. The Makefile content is as follows:

```
MODLIB = $(INSTALL_MOD_PATH)/lib/modules/$(KERNELRELEASE)
export MODLIB

PHONY += prepare0

export extmod_prefix = $(if $(KBUILD_EXTMOD),$(KBUILD_EXTMOD)/)
export MODORDER := $(extmod_prefix)modules.order
export MODULES_NSDEPS := $(extmod_prefix)modules.nsdeps

ifeq ($(KBUILD_EXTMOD),)
core-y      += kernel/ certs/ mm/ fs/ ipc/ security/ crypto/ hello/
core-$(CONFIG_BLOCK)      += block/
core-$(CONFIG_IO_URING) += io_uring/

vmlinux-dirs := $(patsubst %/,%, $(filter %/, \
    $(core-y) $(core-m) $(drivers-y) $(drivers-m) \
    $(libs-y) $(libs-m)))

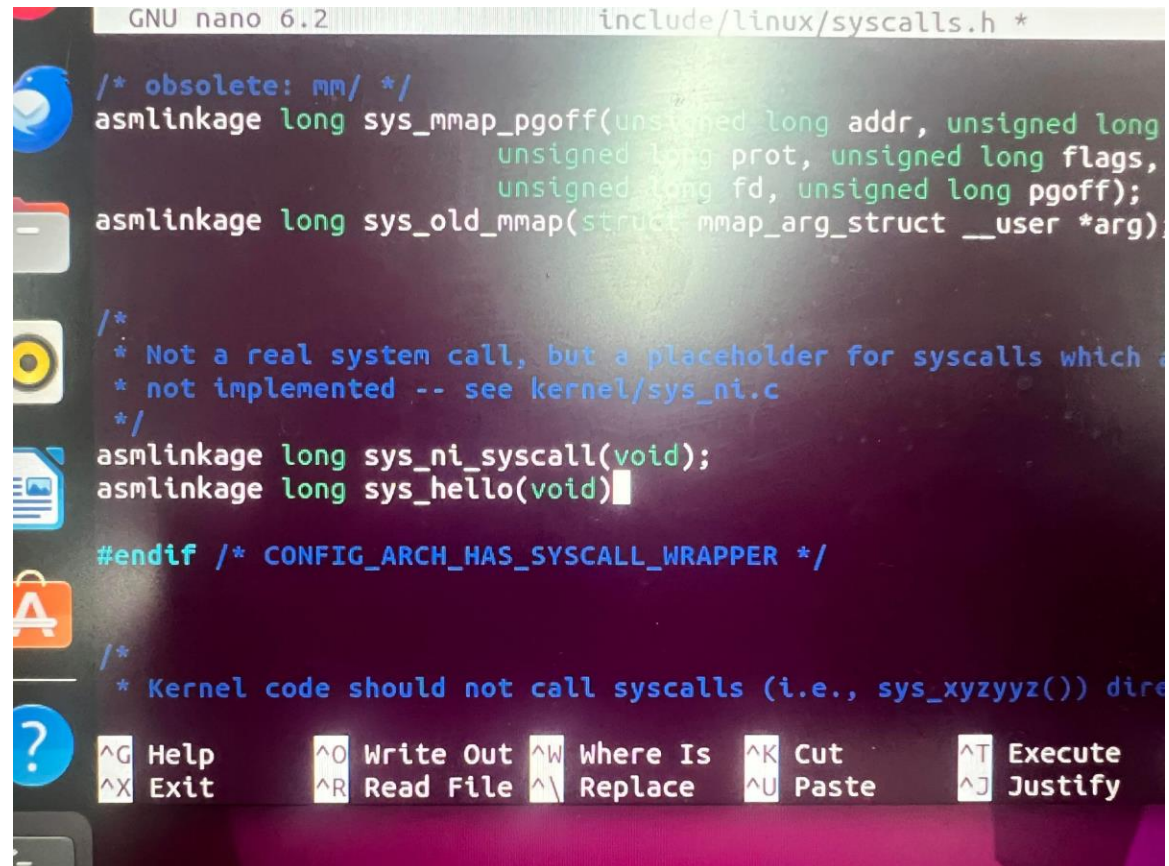
vmlinux-alldirs := $(sort $(vmlinux-dirs) Documentation \
    $(patsubst %/,%, $(filter %/, $(core-)) \
```

The nano editor's help menu is visible at the bottom of the terminal window:

^G Help	^O Write Out	^W Where Is	^K Cut	^T Execute	^C Location
^X Exit	^R Read File	^_ Replace	^U Paste	^J Justify	^_ Go To Line

7.nano include/linux/syscalls.h

- 修改asmlinkage



```
GNU nano 6.2 include/linux/syscalls.h *

/* obsolete: mm/ */
asmlinkage long sys_mmap_pgoff(unsigned long addr, unsigned long
                                unsigned long prot, unsigned long flags,
                                unsigned long fd, unsigned long pgoff);
asmlinkage long sys_old_mmap(struct mmap_arg_struct __user *arg);

/*
 * Not a real system call, but a placeholder for syscalls which are
 * not implemented -- see kernel/sys_ni.c
 */
asmlinkage long sys_ni_syscall(void);
asmlinkage long sys_hello(void)

#endif /* CONFIG_ARCH_HAS_SYSCALL_WRAPPER */

/*
 * Kernel code should not call syscalls (i.e., sys_xyzzyz()) directly
 */

^G Help    ^O Write Out  ^W Where Is  ^K Cut      ^T Execute
^X Exit    ^R Read File  ^\ Replace   ^U Paste    ^J Justify
```


8. 修改system call

```
vboxuser@vboxuser: ~/Downloads/linux-5.19.12
GNU nano 6.2 arch/x86/entry/syscalls/syscall_64.tbl
437 common openat2 sys_openat2
438 common pidfd_getfd sys_pidfd_getfd
439 common faccessat2 sys_faccessat2
440 common process_madvise sys_process_madvise
441 common epoll_pwait2 sys_epoll_pwait2
442 common mount_setattr sys_mount_setattr
443 common quotactl_fd sys_quotactl_fd
444 common landlock_create_ruleset sys_landlock_create_ruleset
445 common landlock_add_rule sys_landlock_add_rule
446 common landlock_restrict_self sys_landlock_restrict_self
447 common memfd_secret sys_memfd_secret
448 common process_mrelease sys_process_mrelease
449 common futex_waitv sys_futex_waitv
450 common set_mempolicy_home_node sys_set_mempolicy_home_node
451 common hello sys_hello
#
# Due to a historical design error, certain syscalls are numbered dif
# in x32 as compared to native x86_64. These syscalls have numbers 5
# Do not add new syscalls to this range. Numbers 548 and above are a
# for non-x32 use.
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C L
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ G
```

9.用report.c

```
/* This file is part of the uapi library, which is licensed under the  
 * MIT license. See the LICENSE file for details.  
 *  
 * This file is a sample program that demonstrates how to use the  
 * uapi library. It is not intended to be used in a production  
 * environment. It is provided as a reference only.  
 *  
 * You must copy the __NR_hello macro from  
 * <your-kernel-build-dir>/arch/x86/include/generated/uapi/asm/unistd.h  
 * In this example, the value of __NR_hello is 548  
 */  
#define __NR_hello 548  
  
int main(int argc, char *argv[]) {  
    int ret = syscall(__NR_hello);  
    assert(ret == 0);  
  
    return 0;  
}
```

Besides, the kernel ring buffer should contain the messages that sys_hello pri

10. result

A screenshot of a terminal window with a dark background. On the left side, there is a vertical dock with several application icons: a yellow circle with a black dot, a blue document icon, an orange shopping bag icon, and a blue circle icon. The terminal text is as follows:

```
[ 5.813577] rfkill: input handler disabled  
[ 5.555783] e1000: enp0s3 NIC Link is Up 1000 Mbps  
RX  
[ 5.556019] IPv6: ADDRCONF(NETDEV_CHANGE): enp0s  
[ 11.176010] kauditd_printk_skb: 9 callbacks supp  
[ 11.176013] audit: type=1400 audit(1698225858.41  
ation="capable" profile="/snap/snapd/20290/usr/lib/  
comm="snap-confine" capability=12 capname="net_adr  
[ 11.176019] audit: type=1400 audit(1698225858.4  
ation="capable" profile="/snap/snapd/20290/usr/lib  
comm="snap-confine" capability=38 capname="perfm  
[ 11.199446] rfkill: input handler enabled  
[ 11.981706] rfkill: input handler disabled  
[ 27.684323] Hello world  
[ 27.684326] 312552052
```